WE CLAIM:

1. A firewall, comprising:

a first port configured for communication with a first device within a first network;

a second port configured for communication with a second device within the first network;

a third port configured for communication between the first network and a second network; and

at least one processor configured to:

determine that a first portion of the incoming packets should be bridged, the first portion having a first source address and a first destination address within the first network;

apply a first screening process to the first portion;

determine that a second portion of the incoming packets should be routed, the second portion having a second source address or a second destination address outside the first network; and

apply a second screening process to the second portion.

2. The firewall of claim 1, wherein the at least one processor is configured to control traffic between the first device and the second device according to a spanning tree protocol.

3. The firewall of claim 1, wherein the at least one processor is configured to control traffic between the first device and the second device according to one or more fields in a layer 2 header of a packet.

4. The firewall of claim 1, wherein the at least one processor is configured to perform an initial check on a packet, wherein the procedures of the initial check are

selected from the group consisting of checking for broadcasting, multicasting and Internet protocol fragments.

5. The firewall of claim 1, wherein the at least one processor is configured to apply the first screening process according to security policies implemented at one or more of layers 3 through 7.

6. The firewall of claim 3, wherein the at least one processor is configured to control traffic between the first device and the second device according to layer 2 access lists applied to one or more fields in the layer 2 header of the packet.

7. The firewall of claim 1, wherein the at least one processor is configured to apply the second screening process according to security policies implemented at one or more of layers 3 through 7.

8. A firewall, comprising:

means for receiving first packets and second packets;

means for determining that the first packets should be bridged, the first packets having a first source address and a first destination address within the first network;

means for applying a first screening process to the first packets;

means for determining that the second packets should be routed; and

means for applying a second screening process to the second packets.

9. A method of implementing a firewall, comprising:

receiving first packets and second packets;

determining that the first packets should be bridged, the first packets having a first source address and a first destination address within the first network;

applying a first screening process to the first packets;

determining that the second packets should be routed; and

applying a second screening process to the second packets.

10. The method of claim 9, wherein the step of determining that the first packets should be bridged comprises performing a bridge lookup based upon media access control address information of the first packets.

11. The method of claim 9, wherein the second screening process comprises performing an access list check.

12. The method of claim 9, wherein the first screening process comprises applying security policies implemented at one or more of layers 3 through 7.

13. A computer program embodied in a machine-readable medium, the computer program comprising instructions for controlling a firewall to perform the following steps:

receive first packets and second packets;

determine that the first packets should be bridged, the first packets having a first source address and a first destination address within the first network;

apply a first screening process to the first packets;

determine that the second packets should be routed; and

apply a second screening process to the second packets.

14. The computer program of claim 13, further comprising instructions for causing the firewall to perform a bridge lookup based upon media access control address information of the first packets.

15. The computer program of claim 13, wherein the instructions for applying the first screening process further comprise instructions for causing the firewall to perform an access list check.

16. The computer program of claim 13, wherein the instructions for applying the second screening process further comprise instructions for causing the firewall to perform an access list check.

17. The firewall of claim 1, further comprising a control plane configured to build a bridge table.

18. The firewall of claim 17, wherein the control plane is further configured to inspect one or more of DHCP, ARP or OSPF packets.

19. The firewall of claim 17, wherein the control plane is further configured to builds a routing table.

20. The firewall of claim 1, further comprising a data plane configured to enforce screening policies.

21. The firewall of claim 20, wherein the data plane is further configured to determine whether to bridge or route packets.

22. The firewall of claim 21, wherein the data plane is further configured to rewrite packet headers before transmitting packets.